

# On the Noether number of $p$ -groups

Kálmán Csiszter

Alfréd Rényi Institute of Mathematics, Hungarian Academy of Sciences  
Reáltanoda u. 13 – 15, 1053 Budapest, Hungary

## Abstract

A group of order  $p^n$  ( $p$  prime) has an indecomposable polynomial invariant of degree at least  $p^{n-1}$  if and only if the group has a cyclic subgroup of index at most  $p$  or it is isomorphic to one of two particular groups of small order.

*Keywords:* polynomial invariants, degree bounds, zero-sum sequences

## 1 Introduction

Let  $G$  be a finite group and  $V$  a  $G$ -module over a field  $\mathbb{F}$  of characteristic which is not dividing the group order  $|G|$ . The Noether-number  $\beta(G, V)$  gives the maximal degree in a minimal generating set of the ring of polynomial invariants  $\mathbb{F}[V]^G$ . It is known that  $\beta(G, V) \leq |G|$  (see [14], [8]). Moreover  $\beta(G) := \sup_V \beta(G, V)$  (where  $V$  runs over all  $G$ -modules over the base field  $\mathbb{F}$ ) is typically much less than  $|G|$ . First it was proved in [17] that  $\beta(G) = |G|$  holds only if  $G$  is cyclic. Then it turned out that  $\beta(G) \leq \frac{3}{4}|G|$  for any non-cyclic group  $G$  (see [7] and [19]). Even more according to [2, Theorem 1.1]  $\beta(G) \geq \frac{1}{2}|G|$  holds if and only if  $G$  has a cyclic subgroup of index at most two, with the exception of four particular groups of small order. Recently some asymptotic extensions of this result were given in [11]. Our goal in the present article is to establish the following strengthening of this kind of results for the class of  $p$ -groups:

**Theorem 1.** *If  $G$  is a finite  $p$ -group for a prime  $p$  and the characteristic of the base field  $\mathbb{F}$  is zero or greater than  $p$  then the inequality*

$$\beta(G) \geq \frac{1}{p}|G| \tag{1}$$

*holds if and only if  $G$  has a cyclic subgroup of index at most  $p$  or  $G$  is the elementary abelian group  $C_2 \times C_2 \times C_2$  or the Heisenberg group of order 27.*

In Section 2 we reduce the proof of our theorem to the study of a single critical case, the Heisenberg group  $H_p$ , which is a group of order  $p^3$  where  $p$  is an odd prime. In Section 3 we deduce the upper bound  $\beta(H_p) < p^2$  for  $p \geq 5$  (see Theorem 12) and finally in Section 4 we show that  $\beta(H_3) = 9$ .

## 2 Reduction of the general case

Recall that for an abelian group  $A$  the Noether number  $\beta(A)$  coincides with the Davenport constant  $D(A)$ , i.e. the maximal length of a zero-sum sequence over  $A$  which does not contain a non-empty, proper zero-sum subsequence (see e.g. [5, Chapter 5]). Its value was calculated for  $p$ -groups in [15]:

$$D(C_{p^{n_1}} \times \cdots \times C_{p^{n_r}}) = \sum_{i=1}^r (p^{n_i} - 1) + 1. \quad (2)$$

The notion of the  $k$ -th Noether number  $\beta_k(G, V)$  (where  $k \geq 1$  and  $\beta_1 = \beta$ ) was introduced in [4, Section 2] in order to estimate the ordinary Noether number from information on its composition factors. This was made possible by [2, Lemma 1.4] according to which for any normal subgroup  $N \triangleleft G$ :

$$\beta(G, V) \leq \beta_{\beta(G/N)}(N, V). \quad (3)$$

When  $A$  is an abelian group  $\beta_k(A)$  coincides with the  $k$ -th Davenport constant  $D_k(A)$  for which we have according to [10, Proposition 5]:

$$D_k(C_p \times C_p) = kp + p - 1. \quad (4)$$

*Proof of Theorem 1.* For  $p = 2$  our claim follows from [2, Theorem 1.1] so for the rest we may assume that  $p \geq 3$ . Let  $G$  be a group of order  $p^n$  for which (1) holds. If  $G$  is non-cyclic then it has a normal subgroup  $N \cong C_p \times C_p$  by [1, Lemma 1.4]. We claim that  $G/N$  must be cyclic. For otherwise by applying [1, Lemma 1.4] to the factor group  $G/N$  we find a subgroup  $K$  such that  $N \triangleleft K \triangleleft G$  and  $K/N \cong C_p \times C_p$ . But then we get using (3) and (4) that

$$\beta(K) \leq \beta_{\beta(C_p \times C_p)}(C_p \times C_p) = p(2p - 1) + p - 1 = 2p^2 - 1 < p^3 = \frac{1}{p}|K|.$$

As  $\beta(G)/|G| \leq \beta(K)/|K|$  by [2, Lemma 1.2] we get a contradiction with (1).

Now let  $g \in G$  be such that  $gN$  generates  $G/N \cong C_{p^{n-2}}$ . Then  $g^{p^{n-2}} \in N$  has order  $p$  or 1. In the first case  $\langle g \rangle$  has index  $p$  in  $G$  and we are done. In the other case  $\langle g \rangle \cap N = \{1\}$  hence  $G \cong N \rtimes \langle g \rangle$ . If  $g$  acts trivially on  $N$  then  $G$  contains a subgroup  $H \cong C_p \times C_p \times C_p$  for which we have

$\beta(H) = 3p - 2$  by (2) hence  $\beta(G)/|G| \leq \beta(H)/|H| < 3/p^2 \leq 1/p$  as  $p \geq 3$ , a contradiction. This shows that  $g$  must act non-trivially on  $C_p \times C_p$ . It is well known that  $\text{Aut}(C_p \times C_p) = \text{GL}(2, p)$  has order  $(p^2 - 1)(p^2 - p)$  so its Sylow  $p$ -subgroup must have order  $p$  and it is isomorphic to  $C_p$ . Therefore if  $n \geq 4$  then  $g^p \neq 1$  must act trivially on  $N$  and we get again a subgroup  $H = C_p \times C_p \times C_p$  as before, which was excluded. The only case which remains open is that  $n = 3$  and  $G \cong (C_p \times C_p) \rtimes C_p$  where the factor  $C_p$  acts non-trivially on  $C_p \times C_p$ . This is the Heisenberg group which we will denote by  $H_p$ . We will prove below (see Theorem 12) that  $\beta(H_p) < p^2$  for all  $p > 3$  under our assumption on the characteristic of the base field  $\mathbb{F}$ . So among the Heisenberg groups the inequality (1) can only hold for  $H_3$ . This proves the “only if” part of the theorem. For the converse: for any cyclic subgroup  $C \leq G$  we have  $\beta(G) \geq \beta(C) = |C| = |G|/[G : C]$  by [17, Proposition 5.1] moreover  $\beta(C_2^3) = 4$  by (2) and  $\beta(H_3) = 9$  by Corollary 15.  $\square$

**Remark 2.** The precise value of the Noether number for all  $p$ -groups which satisfy (1) according to Theorem 1 is already known. We have equality in (1) for  $C_2^3$  and  $H_3$  by (2) and Corollary 15, respectively. For the rest, the groups of order  $p^n$  which have a cyclic subgroup of index  $p$  were classified by Burnside (see e.g. [1, Theorem 1.2]) as follows:

- (i) if  $G$  is abelian, then either  $G$  is cyclic with  $\beta(G) = p^n$  or  $G = C_{p^{n-1}} \times C_p$  in which case it has  $\beta(G) = p^{n-1} + p - 1$  by (2)
- (ii) if  $G$  is non-abelian and  $p > 2$  then  $G$  is isomorphic to the modular group  $M_{p^n} \cong C_{p^{n-1}} \rtimes C_p$ . We have  $\beta(M_{p^n}) = p^{n-1} + p - 1$  by [3, Remark 10.4].
- (iii) if  $G$  is non-abelian and  $p = 2$  then  $G$  is the dihedral group  $D_{2^n}$  or the semi-dihedral group  $SD_{2^n}$  or the generalised quaternion group  $Q_{2^n}$ . We have  $\beta(Q_{2^n}) = 2^{n-1} + 2$  and  $\beta(D_{2^n}) = \beta(SD_{2^n}) = 2^{n-1} + 1$  by [17, Theorem 7.1], [19, Proposition 13] or [3, Theorem 10.3].

### 3 The Heisenberg group $H_p$

The Heisenberg group  $H_p = \langle a, b \rangle$  can be defined by the presentation:

$$a^p = b^p = c^p = 1 \quad [a, b] = c \quad [a, c] = [b, c] = 1 \quad (5)$$

where  $[a, b]$  denotes the commutator  $a^{-1}b^{-1}ab$ . The subgroups  $A := \langle a, c \rangle$  and  $B := \langle b, c \rangle$  are normal, isomorphic to  $C_p \times C_p$ , and they are the only maximal subgroups of  $H_p$ . Therefore the Frattini-subgroup, the center, and the derived subgroup of  $H_p$  all coincide with  $\langle c \rangle$ , so that  $H_p$  is extraspecial. It is easily seen that  $H_p/\langle c \rangle$  is also isomorphic to  $C_p \times C_p$ . Taking into account

only the subgroup structure of  $H_p$  the best upper bound that we can give about its Noether number by means of (3) and (4) is the following:

$$\beta(H_p) \leq \beta_{\beta(C_p)}(C_p \times C_p) = p^2 + p - 1. \quad (6)$$

Our goal in this section is to enhance this estimate by analysing more closely the invariant rings of certain  $H_p$ -modules.

The irreducible  $H_p$ -modules over a field  $\mathbb{F}$  with  $\text{char}(\mathbb{F}) \neq p$  are of two types. Composing any character of  $H_p/\langle c \rangle \cong C_p \times C_p$  with the canonic surjection  $H_p \rightarrow H_p/\langle c \rangle$  gives  $p^2$  non-isomorphical 1-dimensional irreducible representations of  $H_p$ . The second kind of irreducible representations are obtained in the following way: for every primitive  $p$ -th root of unity  $\omega \in \mathbb{F}$  take the induced representation  $V_\omega := \text{Ind}_A^{H_p} \langle v \rangle$ , where  $\langle v \rangle$  is a 1-dimensional left  $A$ -module such that  $a \cdot v = v$  and  $c \cdot v = \omega v$ . In the normal basis  $\{v, b \cdot v, \dots, b^{p-1} \cdot v\}$  this representation is then given in terms of matrices as

$$a \mapsto \begin{pmatrix} 1 & & & \\ & \omega & & \\ & & \ddots & \\ & & & \omega^{p-1} \end{pmatrix} \quad b \mapsto \begin{pmatrix} 0 & \cdots & \cdots & 1 \\ 1 & & & \vdots \\ & \ddots & & \vdots \\ & & 1 & 0 \end{pmatrix} \quad c \mapsto \omega I_p. \quad (7)$$

where  $I_p$  is the  $p \times p$  identity matrix. Each  $V_\omega$  is irreducible by Mackey's criterion (see e.g. [18]) and for  $\omega' \neq \omega$  it is easily seen (e.g. from the matrix corresponding to  $c$ ) that  $V_\omega$  and  $V_{\omega'}$  are non-isomorphical. Adding the squares of the dimensions of the above irreducible  $H_p$ -modules we get  $p^2 \cdot 1 + (p-1)p^2 = p^3 = |H_p|$ , hence no other irreducible  $H_p$ -modules exist. So an arbitrary  $H_p$ -module  $W$  has the direct sum decomposition

$$W = V_\omega^{n_1} \oplus \cdots \oplus V_{\omega^{p-1}}^{n_{p-1}} \oplus U \quad (8)$$

for some integers  $n_i \geq 0$ , where  $U$  consists only of 1-dimensional irreducible representations with  $\langle c \rangle$  in their kernel, while  $V_i := V_{\omega^i}^{n_i}$  is an isotypic component consisting of  $n_i$  copies of  $V_{\omega^i}$ .

When speaking of a coordinate ring  $\mathbb{F}[V_{\omega^i}] = \mathbb{F}[x_1, \dots, x_p]$  we will always tacitly assume that the variables form a dual basis of the normal basis given at (7) and that  $H_p$  acts on them from the right:  $x^g(v) = x(g \cdot v)$  for all  $g \in H_p$ . For any such variable  $x \in \mathbb{F}[V_{\omega^i}]$  there is a character  $\chi \in \text{Hom}(A, \mathbb{F}^\times)$  such that  $x^g = \chi(g)x$  for all  $g \in A$ . This character will be called *the weight* of  $x$  and we denote it by  $\phi(x) := \chi$ . We will use the additive notation for the group of characters  $\hat{A} = \text{Hom}(A, \mathbb{F}^\times)$ . We will tacitly use the well known fact that  $\hat{A} \cong A$ .

Consider also the canonic projections  $\pi_a : \text{Hom}(A, \mathbb{F}^\times) \rightarrow \text{Hom}(\langle a \rangle, \mathbb{F}^\times)$  respectively  $\pi_c : \text{Hom}(A, \mathbb{F}^\times) \rightarrow \text{Hom}(\langle c \rangle, \mathbb{F}^\times)$ . We write  $\phi_c(x) = \pi_c(\phi(x))$  and similarly  $\phi_a(x) = \pi_a(\phi(x))$ . To any monomial  $m = x_1 \cdots x_n$  we will associate its *weight sequence*  $\Phi(m) := (\phi(x_1), \dots, \phi(x_n))$ . We also define the projections  $\Phi_c(m) := (\phi_c(x_1), \dots, \phi_c(x_n))$  and  $\Phi_a(m)$  analogously. The sum of any sequence  $S$  is denoted by  $\sigma(S)$  and we also write  $\phi(m) = \sigma(\Phi(m))$ .

By our conventions for any variable  $x \in \mathbb{F}[W]$  we have  $\phi_c(x) = 0$  if and only if  $x$  belongs to  $\mathbb{F}[U]$ , and otherwise the value  $\phi_c(x) \neq 0$  identifies the isotypic component  $V_i$  to which  $x$  belongs. Moreover we see from (7) that  $\phi_a(x^{b^n}) = \phi_a(x) + n \cdot \phi_c(x)$ . We will frequently use the consequence of this observation that for any variable  $x$  with  $\phi_c(x) \neq 0$  and any arbitrarily given  $\theta \in \text{Hom}(\langle a \rangle, \mathbb{F}^\times)$  there is always an element  $g \in \langle b \rangle$  such that  $\phi_a(x^g) = \theta$ .

We will choose as a starting point of our argument an easy proof of a well known fact (see [12, Theorem 2.1] or [6, Lemma 3.8.1]) adapted to the more particular context which is relevant for us here:

**Lemma 3.** *Let  $G$  be a finite group with a normal subgroup  $N$  such that  $G/N$  is abelian. Let  $W$  be a  $G$ -module over an algebraically closed field  $\mathbb{F}$  such that  $|G| \in \mathbb{F}^\times$ . Then  $(\mathbb{F}[W]_+^N)^k \subset \mathbb{F}[W]_+^G \mathbb{F}[W]$  for any  $k \geq D(G/N)$ .*

*Proof.* Let  $\mathbb{F}[W]^{G,\chi}$  denote the  $\mathbb{F}[W]^G$ -module of  $G$ -semi-invariants of weight  $\chi \in \text{Hom}(G, \mathbb{F}^\times)$ . Regarded as a  $G/N$ -module  $\mathbb{F}[W]^N$  has the direct sum decomposition  $\bigoplus_{\chi \in \widehat{G/N}} \mathbb{F}[W]^{G,\chi}$ . The projections  $\tau_\chi : \mathbb{F}[W]^N \rightarrow \mathbb{F}[W]^{G,\chi}$  are defined by the formula  $\tau_\chi(u) = \sum_{g \in G/N} \chi^{-1}(g)u^g$ . (Here we needed our assumptions on  $\mathbb{F}$ .) Now for any  $u_1, \dots, u_k \in \mathbb{F}[W]_+^N$  we have:

$$\prod_{i=1}^k u_i = \prod_{i=1}^k \left( \sum_{\chi \in \widehat{G/N}} \tau_\chi(u_i) \right) = \sum_{\chi_1, \dots, \chi_k \in \widehat{G/N}} \tau_{\chi_1}(u_1) \cdots \tau_{\chi_k}(u_k) \quad (9)$$

The term  $\tau_{\chi_1}(u_1) \cdots \tau_{\chi_k}(u_k)$  belongs to the ideal  $\mathbb{F}[W]_+^G \mathbb{F}[W]$  whenever the sequence  $(\chi_1, \dots, \chi_k)$  contains a zero-sum subsequence. But this happens for all terms in (9) provided that  $k \geq D(G/N)$ .  $\square$

**Lemma 4.** *If in Lemma 3 we have  $G/N \cong C_p$  for some prime  $p \geq 3$  then for any  $g \in G/N$  and any elements  $u_1, \dots, u_{p-1} \in \mathbb{F}[W]_+^N$  we have the relation:*

$$u_1 \cdots u_{p-1} - u_1^g u_2^{-g} u_3 \cdots u_{p-1} \in \mathbb{F}[W]_+^G \mathbb{F}[W].$$

*Proof.* Observe that in (9) the sequence  $(\chi_1, \dots, \chi_{p-1})$  over  $\hat{C}_p$  is zero-sum free if and only if  $\chi_1 = \dots = \chi_{p-1}$ . As a result we get:

$$u_1 \cdots u_{p-1} \in \sum_{\chi \in \widehat{G/N}} \tau_\chi(u_1) \cdots \tau_\chi(u_{p-1}) + \mathbb{F}[W]_+^G \mathbb{F}[W]. \quad (10)$$

Replacing here  $u_1$  and  $u_2$  with  $u_1^g$  and  $u_2^{-g}$ , respectively, and observing that by the defining formula of  $\tau_\chi$  we have  $\tau_\chi(a^g) = \chi(g)\tau(a)$  for any  $a \in \mathbb{F}[W]^N$  we infer that  $u_1^g u_2^{-g} u_3 \cdots u_{p-1}$  belongs to the same residue class modulo the ideal  $\mathbb{F}[W]_+^G \mathbb{F}[W]$  to which  $u_1 \cdots u_{p-1}$  does belong. This proves our claim.  $\square$

Let us introduce some notation related to sequences over an abelian group  $A$  which are in concordance with the usage in [9]. For any sequence  $S$  and any  $e \in A$  we denote by  $\mathbf{v}_e(S)$  the multiplicity of the element  $e$  in  $S$ . Furthermore set  $h(S) := \max_{e \in A} \mathbf{v}_e(S)$ . Let  $\Sigma(S)$  denote the set of all partial sums of  $S$ , that is to say  $\Sigma(S) = \{\sigma(T) : T \subset S\}$ . If  $S$  contains only non-zero elements of the group  $C_p$  then by the repeated use of the Cauchy-Davenport theorem (see [9, Corollary 5.2.8.1]) we get

$$|\Sigma(S)| \geq \min\{p, |S| + 1\}. \quad (11)$$

For the rest of this Section let  $G$  denote a Heisenberg group  $H_p$ .

**Lemma 5.** *Let  $m \in \mathbb{F}[W]^A$  be a monomial such that  $\deg(m) \geq p^2$  and  $\mathbf{v}_0(\Phi_c(m)) \leq p - 1$ . Let  $\Phi_c(m) = S_1 \cdots S_k T$  where  $k \leq p - 2$  and each  $S_i$  is an irreducible zero-sum sequence over  $C_p \setminus \{0\}$  of length  $0 < |S_i| \leq p - 1$ . Then either  $m \in \mathbb{F}[W]_+^G \mathbb{F}[W]_+$  or there are monomials  $u_1, \dots, u_k, v \in \mathbb{F}[W]_+^A$  such that  $\Phi_c(u_i) = S_i$  for all  $i = 1, \dots, k$  and  $m - u_1 \cdots u_k v \in \mathbb{F}[W]_+^G \mathbb{F}[W]_+$ .*

*Proof.* We use induction on  $k$ . The case  $k = 0$  being trivial assume  $k \geq 1$ . By induction we have monomials  $u_1, \dots, u_{k-1}, v \in \mathbb{F}[W]_+^A$  with the required properties. Then  $\deg(v) \geq p^2 - (k - 1)(p - 1) > (p - k + 1)p - 1 = D_{p-k}(A)$  by (4) hence a factorisation  $v = v_1 \cdots v_{p-k+1}$  exists with  $v_i \in \mathbb{F}[W]_+^A$  for all  $i$ . As  $S_k \subset \Phi_c(v)$  there is a monomial  $w \mid v$  such that  $\Phi_c(w) = S_k$ . For  $k = 1$  we may even assume that  $w \mid v_2 \cdots v_p$  as  $|S_1| \leq p - 1$ . We have two cases:

(i) if  $w$  is “scattered” in the sense that  $w = w_1 \cdots w_n$  where  $n \geq 2$  and for all  $t = 1, \dots, n$  we have  $w_t \in \mathbb{F}[W]_+$  and  $w_t \mid v_{i_t}$  for some indices  $i_1 < \dots < i_n$ : then as  $\phi_c(w_1) \neq 0$  there is a  $g \in \langle b \rangle$  such that  $\phi_a(w_1^g) = -\phi_a(w_2 \cdots w_n)$ . Now set  $m' = u_1^{-g} \cdots u_{k-1} v_1 \cdots v_{i_1}^g \cdots v_{p-k+1}$  if  $k > 1$  or  $m' = v_1^{-g} v_2 \cdots v_{i_1}^g \cdots v_p$  for  $k = 1$ . Then  $m - m' \in \mathbb{F}[W]_+^G \mathbb{F}[W]_+$  by Lemma 4 and  $m'$  contains the product of the  $A$ -invariant monomials  $u_1^{-g}, u_2, \dots, u_{k-1}, u_k := w_1^g w_2 \cdots w_n$  which satisfy the requirement on their weight sequences, so we are done.

(ii) Otherwise, when  $w$  is not scattered by any factorisation of  $v$ , assume first that  $k > 1$ . We may also assume that  $w \mid v_2$  and that  $\deg(v_2) \leq D(A) = 2p - 1$ , for otherwise  $v_2 \in (\mathbb{F}[W]_+^A)^2$ , whence  $m \in (\mathbb{F}[W]_+^A)^{p+1} \subset \mathbb{F}[W]_+^G \mathbb{F}[W]_+$  by Lemma 3. Therefore  $\deg(v/v_2) \geq p^2 - (k - 1)(p - 1) - (2p - 1) \geq 2p - 2$ , as  $k \leq p - 2$ . Let  $\Phi_c(v/v_2) = R(0^s)$  where  $0 \notin R$ . As  $s \leq p - 1$  by assumption we have then  $|R| \geq p - 1$  hence  $|\Sigma(R)| = p$  by (11). So for

any variable  $x \mid w$  there is a monomial  $r \mid (v/v_2)$  such that  $\phi_c(x) = -\phi_c(r)$ . Moreover as  $\phi_c(x) \neq 0$  there is a  $g \in \langle b \rangle$  such that  $\phi_a(x^g) = -\phi_a(r)$ . Now consider the monomial  $m' = u_1^{-g} \cdots u_{k-1} v_1 v_2^g \cdots v_{p-k+1}$ . This is well defined as  $k > 1$  and we have  $m - m' \in \mathbb{F}[W]_+^G \mathbb{F}[W]_+$  by Lemma 4. Let  $v'_1 = x^g r$  and observe that  $\deg(m'/u_1^{-g} \cdots u_{k-1} v'_1) \geq p^2 - kp > D_{p-k-1}(A)$  so that we can find monomials  $v'_2, \dots, v'_{p-k+1} \in \mathbb{F}[W]_+^A$  such that  $m' = u_1 \cdots u_{k-1} v'_1 \cdots v'_{p-k+1}$ . Moreover  $w' := wx^g/x$  is scattered by this factorisation since by construction  $x^g \mid v'_1$  while  $w'/x^g$  is contained in  $v'_2 \cdots v'_{p-k+1}$ . Hence  $m'$  falls under case (i) and we are done taking into account that  $\Phi_c(w') = \Phi_c(w)$ .

Finally we deal with the case  $k = 1$  along the same argument but with some modifications. We assume that  $\deg(v_1 v_2) \leq D_2(A) = 3p-1$  as otherwise again  $m \in (\mathbb{F}[W]_+^A)^{p+1} \subset \mathbb{F}[W]_+^G \mathbb{F}[W]_+$  by Lemma 3. As a result we have  $\deg(v/v_1 v_2) \geq p^2 - 3p + 1 \geq 2p + 1$  as  $p \geq 5$ . Then  $\Phi_c(v/v_1 v_2) = R(0^s)$  where  $s \leq p-1$  and  $|R| \geq p+1$  so that  $|\Sigma(R)| = p$ . Then for any variable  $x \mid v_2$  there is a monomial  $r \mid v/v_1 v_2$  such that  $\phi_c(x) = -\phi_c(r)$ . Then for the monomial  $m' = v_1^{-g} v_2^g \cdots v_p$  we have  $m - m' \in \mathbb{F}[W]_+^G \mathbb{F}[W]_+$  by Lemma 4. Let  $v'_i = x^g r$  and take a factorisation  $m' = v'_1 v'_2 \cdots v'_p$  as before. Then  $w' := wx^g/x$  is scattered by this factorisation so we get case i) again.  $\square$

**Lemma 6.** *Let  $S$  be a sequence of elements of  $C_p$  such that  $|S| \geq p$  and  $|S| - h(S) \geq \frac{p+1}{2}$ . If  $S = RT$  where  $R$  is a non-empty zero-sum subsequence of  $S$  of minimal length then either  $|R| \leq \frac{p-1}{2}$  or else  $|R| = \frac{p+1}{2}$  and  $h(T) < h(S)$ .*

*Proof.* Set  $m := \frac{p-1}{2}$  and assume that  $|R| > m$ . Fix an enumeration  $e_1, \dots, e_p$  of the elements of  $C_p$  such that  $\mathbf{v}_{e_1}(S) \geq \cdots \geq \mathbf{v}_{e_p}(S)$ ; for simplicity we will write  $\mathbf{v}_i$  instead of  $\mathbf{v}_{e_i}$ . For any  $r \geq 0$  we define the truncated sequence  $S^{[r]} \subset S$  by setting  $\mathbf{v}_i(S^{[r]}) = \min\{r, \mathbf{v}_i(S)\}$  for all  $i = 1, \dots, p$ . According to [9, Theorem 5.7.3] any sequence  $T$  over  $C_p$  with length  $|T| \geq p$  contains a non-empty zero-sum subsequence of length at most  $h(T)$ . This implies that we must have  $|S^{[m]}| < p$  for otherwise  $|R| \leq m$  would follow from the cited result. But  $|S| \geq p$  by assumption, whence  $S^{[m]} \neq S$ . This is only possible if  $h(S) > m$ . As a result we have  $h(S^{[m]}) = \mathbf{v}_1(S^{[m]}) = m$  and therefore  $\sum_{i=2}^p \mathbf{v}_i(S^{[m]}) = |S^{[m]}| - h(S^{[m]}) \leq p - 1 - m = m$ . On the other hand  $\sum_{i=2}^p \mathbf{v}_i(S) = |S| - h(S) > m$  by our assumption. This is only possible if  $\mathbf{v}_2(S) > m$ , because otherwise we would have  $\mathbf{v}_i(S^{[m]}) = \mathbf{v}_i(S)$  for all  $i \geq 2$ . But then  $\mathbf{v}_1(S^{[m]}) = \mathbf{v}_2(S^{[m]}) = m$  hence the assumption  $|S^{[m]}| < p$  enforces that  $\mathbf{v}_3(S^{[m]}) = 0$ . Finally this implies that  $\mathbf{v}_3(S) = 0$ .

Now by what has been proven so far we have  $|S^{[m+1]}| \geq 2(m+1) = p+1$  whence  $|R| = m+1$  by [9, Theorem 5.7.3]. Moreover  $R$  is of the form  $(e_1^k e_2^{m+1-k})$  for some  $k \geq 0$  as  $\mathbf{v}_3(S) = 0$ . Here  $k = 0$  or  $k = m+1$  are both impossible since  $e_i^{m+1}$  is not a zero-sum sequence for  $i = 1, 2$ . Consequently  $h(T) \leq h(S) - \min\{k, m+1-k\} < h(S)$ .  $\square$



**Lemma 7.** *Let  $p \geq 3$  and let  $S$  be a zero-sum sequence over  $C_p$  with  $|S| \geq p^2$  and  $h(S) \leq (p-1)^2$ . Then one of the following holds:*

- (a)  *$S$  factors into at least  $2p$  non-empty zero-sum sequences, or*
- (b)  *$\mathbf{v}_0(S) \leq p-1$  and  $S \supset S_1 \cdots S_k$ , where  $2 \leq k \leq 3$ , each  $S_i$  is an irreducible zero-sum sequence over  $C_p \setminus \{0\}$  of length  $0 < |S_i| \leq p-1$  and moreover  $|S_1 \cdots S_k| \leq (k-1)p$ .*

*Proof.* Let  $\ell(S)$  denote the maximum number of non-empty zero-sum sequences into which  $S$  can be factored. Assume  $\ell(S) < 2p$ ; then we have:

$$2p-1 \geq \ell(S) \geq \mathbf{v}_0(S) + \frac{1}{p}(|S| - \mathbf{v}_0(S)) \geq \frac{p-1}{p}\mathbf{v}_0(S) + p.$$

whence  $\mathbf{v}_0(S) \leq p$  follows. Consider now the case  $\mathbf{v}_0(S) = p$ . Let  $S = S'(0^p)$  where  $0 \notin S'$ . Then by our assumptions  $|S'| \geq p(p-1)$  while  $\ell(S') \leq p-1$ . It is easily seen that this is only possible if  $S' = (e^{p(p-1)})$  for some  $e \in C_p \setminus \{0\}$ . But then  $h(S) = p(p-1)$  contrary to our assumption on  $h(S)$ . From this we conclude that  $\mathbf{v}_0(S) \leq p-1$ .

Let  $S' = S_1 \cdots S_n$  be a factorisation such that each  $S_i$  is a non-empty zero-sum subsequence of minimal length in  $T_i := S_i \cdots S_n$  for all  $i = 1, \dots, n$ . Given that  $|T_1| = |S| - \mathbf{v}_0(S) \geq p^2 - p + 1$  we have  $|T_1| - h(T_1) \geq p$  hence  $|S_1| \leq \frac{p+1}{2}$  according to Lemma 6. We will consider now the following cases:

(i) if  $|S_1| \leq \frac{p-1}{2}$  then  $|T_2| \geq |T_1| - \frac{p-1}{2} \geq p$  on the one hand and in the same time  $|T_2| - h(T_2) \geq |T_1| - \frac{p-1}{2} - h(T_1) \geq \frac{p+1}{2}$  by our assumptions. Hence we have  $|S_2| \leq \frac{p+1}{2}$  by Lemma 6. Then  $|S_1 S_2| \leq p$  and we get case (b).

(ii) if  $|S_1| = \frac{p+1}{2}$  then again by Lemma 6 we have  $h(T_2) \leq h(T_1) - 1$ . So this time  $|T_2| = |T_1| - \frac{p+1}{2} \geq p$  and  $|T_2| - h(T_2) \geq |T_1| - \frac{p+1}{2} - h(T_1) + 1 \geq \frac{p+1}{2}$ . Taking into account that  $|S_2| \geq |S_1|$  by construction, we have  $|S_2| = \frac{p+1}{2}$  by Lemma 6. Moreover the same Lemma 6 assures that  $h(T_3) \leq h(T_2) - 1$ . As a result  $|T_3| - h(T_3) \geq |T_2| - \frac{p+1}{2} - h(T_2) + 1 \geq 1$ . In the same time we also have  $|T_3| = |S| - \mathbf{v}_0(S) - |S_1 S_2| \geq p^2 - 2p \geq p$ . Consider now the truncated sequence  $T_3^{[p-1]}$ . Given that  $h(T_3) < |T_3|$  we must have  $|T_3^{[p-1]}| \geq p$ , too. Then again by [9, Theorem 5.7.3] we conclude that  $|S_3| \leq p-1$ , so that  $|S_1 S_2 S_3| \leq 2p$  and we get case (b) with  $k = 3$ .  $\square$

**Proposition 8.** *Let  $p \geq 5$ . If a monomial  $m \in \mathbb{F}[W]^A$  has  $\deg(m) \geq p^2$  and  $h(\Phi_c(m)) \leq (p-1)^2$  then  $m \in \mathbb{F}[W]_+^G \mathbb{F}[W]_+$ .*

*Proof.* We can apply Lemma 7 to the sequence  $S := \Phi_c(m)$ . In case (a) it follows that  $m \in (\mathbb{F}[W]_+^c)^{2p}$ . But  $(\mathbb{F}[W]_+^c)^{2p-1} \subset \mathbb{F}[W]_+^G \mathbb{F}[W]$  by Lemma 3, whence the claim. In case (b) we have a factorisation  $S = S_1 \cdots S_k T$  which satisfies all the requirements of Lemma 5, as  $k \leq 3 \leq p-2$ . In addition we also



have  $|S_1 \cdots S_k| \leq (k-1)p$ . It follows that monomials  $u_1, \dots, u_k, v \in \mathbb{F}[W]_+^A$  exist with  $\Phi_c(u_i) = S_i$  such that  $m - m' \in \mathbb{F}[W]_+^G \mathbb{F}[W]_+$  for  $m' := u_1 \cdots u_k v$ . Of course  $\deg(m) = \deg(m')$  also holds by construction. It follows that  $\deg(v) = \deg(m) - \deg(u_1 \cdots u_k) \geq (p-k+1)p > D_{p-k}(A)$  by (4). As a result then  $v \in (\mathbb{F}[W]_+^A)^{p-k+1}$  and  $m' \in (\mathbb{F}[W]_+^A)^{p+1} \subset \mathbb{F}[W]_+^G \mathbb{F}[W]_+$  by Lemma 3 and this proves our claim.  $\square$

We will also need some further results from additive combinatorics. We denote by  $\eta(A)$  the smallest length of a sequence  $S$  over  $A$  which guarantees the existence of a zero-sum subsequence  $T \subset S$  of length  $0 < |T| \leq \exp(A)$ . For the particular case  $A = C_p^2$  its value was established in [16, Lemma 1.1]:

$$\eta(C_p^2) = 3p - 2. \quad (12)$$

Given any sequences  $T \subset R$  we denote by  $RT^{-1}$  the unique sequence  $Q$  such that  $R = TQ$ .

**Lemma 9.** *Let  $p \geq 5$ . Let  $S$  be a zero-sum sequence over  $\langle a, c \rangle \cong C_p \times C_p$  with  $|S| \geq p^2$  and with a subsequence  $R \subset S$  such that  $|R| > (p-1)^2$  and  $\pi_c(R) = e^{|R|}$  for some non-identity element  $e \in \langle c \rangle$ . Then for any  $T \subset R$  with  $|T| \leq p-1$  there is a factorisation  $S = S_1 \cdots S_p$  into non-empty zero-sum sequences  $S_i$  such that  $T \subset S_3 \cdots S_p$  and  $f \in S_1 S_2$  for some  $f \in R$ .*

*Proof.* We have  $|RT^{-1}| \geq (p-2)(p-1) + 1 \geq 3p-2 = \eta(C_p^2)$  by (12) as  $p \geq 5$ . So there is a zero-sum sequence  $S_1 \subset RT^{-1}$  with  $|S_1| \leq p$ . Then  $|SS_1^{-1}T^{-1}| \geq p^2 - 2p + 1 \geq 3p+1 > \eta(C_p^2)$  again by (12), so we have another zero-sum sequence  $S_2 \subset SS_1^{-1}T^{-1}$  with  $|S_2| \leq p$ . Finally observe that  $|SS_1^{-1}S_2^{-1}| \geq p^2 - 2p > D_{p-3}(C_p^2) = p^2 - 2p - 1$  by (4) which yields a factorisation  $SS_1^{-1}S_2^{-1} = S_3 \cdots S_p$  into non-empty zero-sum sequences  $S_3, \dots, S_p$ . Now we are done, since by construction  $T \subset SS_1^{-1}S_2^{-1}$  and  $S_1 \subset R$ .  $\square$

From now on we assume for simplicity that in the direct sum decomposition (8) we have  $n_1 = \dots = n_{p-1} = n$  for some  $n \geq 1$ , as any other  $G$ -module can be embedded in one of this kind. That is to say we have an isotypic decomposition  $W = V_1 \oplus \dots \oplus V_{p-1} \oplus U$  where  $V_i = V_{i,1} \oplus \dots \oplus V_{i,n} \cong V_{\omega^i}^{\oplus n}$  for all  $i = 1, \dots, p-1$ . For any monomial  $m \in \mathbb{F}[W]$  the isomorphism  $\mathbb{F}[W] \cong \bigotimes_{i=1}^{p-1} \bigotimes_{j=1}^n \mathbb{F}[V_{i,j}] \otimes \mathbb{F}[U]$  yields a factorisation  $m = \prod_{i=1}^{p-1} \prod_{j=1}^n m_{i,j} u$ . We also write  $m = m_1 \cdots m_{p-1} u$  where  $m_i = \prod_{j=1}^n m_{i,j}$  for all  $i = 1, \dots, p-1$ . The multidegree of  $m$  is the matrix  $\underline{\deg}(m) := [\deg(m_{i,j})]_{1 \leq i \leq p-1, 1 \leq j \leq n}$ .

**Lemma 10.** *Assume  $p \geq 5$ . Let  $m \in \mathbb{F}[W]^A$  be a monomial such that  $\deg(m) \geq p^2$  and  $\deg(m_1) > (p-1)^2$ . Then for any monomial  $w \in \mathbb{F}[V_1]$  such that  $\deg(w) \leq p$  and  $\underline{\deg}(w) \leq \underline{\deg}(m_1)$  there is a monomial  $v \in \mathbb{F}[W]$  such that  $m - vw \in \mathbb{F}[W]_+^G \mathbb{F}[W]_+$ .*

*Proof.* We use induction on the degree of the monomial  $w' := \gcd(w, m)$ . If  $\deg(w') = \deg(w)$  then  $w \mid m$  and we are done. So for the rest assume that  $\deg(w') < \deg(w)$ . Fix some variable  $x$  dividing  $w/w'$ . We can apply Lemma 9 for the sequences  $S = \Phi(m)$ ,  $R = \Phi(m_1)$  and  $T = \Phi(w')$ . This yields a factorisation  $m = u_1 \cdots u_p$  with  $u_i \in \mathbb{F}[W]_+^A$  such that  $w' \mid u_3 \cdots u_p$  and  $u_1 u_2$  contains a variable  $y \in \mathbb{F}[V_1]$ . For the rest we may assume by symmetry that  $y \mid u_1$ . We have two cases:

(i) If  $x$  and  $y$  belong to the same coordinate ring  $\mathbb{F}[V_{1,j}]$  then there is a  $g \in \langle b \rangle$  such that  $y^g = x$ . Now for the monomial  $m' := u_1^g u_2^{g^{-1}} u_3 \cdots u_p$  observe that  $\gcd(w, m')$  contains  $w'x$ . Hence  $m' - wv \in \mathbb{F}[W]_+^G \mathbb{F}[W]_+$  for a monomial  $v \in \mathbb{F}[W]$  by the induction hypothesis, while  $m - m' \in \mathbb{F}[W]_+^G \mathbb{F}[W]_+$  holds by Lemma 4 and we are done.

(ii) otherwise: since by assumption  $\deg(w') < \deg(w) \leq \deg(m_1)$  there must still be a variable  $z$  in  $m_1/w'$  which belongs to the same coordinate ring  $\mathbb{F}[V_{1,j}]$  as  $x$ . If  $z \mid u_1 u_2$  then by replacing  $y$  with  $z$  we get back to case (i). So for the rest we may assume without loss of generality that  $z \mid u_3$ . Now  $y \in \mathbb{F}[V_{1,k}]$  for some  $k \neq j$  but since  $y$  and  $z$  belong to the same isotypic component  $V_1$  there is a  $g \in \langle b \rangle$  such that  $\phi(y^g) = \phi(z)$ . Replace  $m$  by the monomial  $m'' := u_1^g u_2^{g^{-1}} u_3 \cdots u_p$  again by Lemma 4. After exchanging  $y^g$  and  $z$  in the monomials  $u_1^g$  and  $u_3$  case (i) applies to  $m''$  and we are done.  $\square$

**Proposition 11.** *Let  $p \geq 5$  and assume that  $\text{char}(\mathbb{F})$  is 0 or greater than  $p$ . If a monomial  $m \in \mathbb{F}[W]^A$  has  $\deg(m) \geq p^2$  and  $h(\Phi_c(m)) > (p-1)^2$  then  $m \in \mathbb{F}[W]_+^G \mathbb{F}[W]_+$ .*

*Proof.* Assume that in the factorisation  $m = m_1 \cdots m_{p-1} u$  where  $m_i \in \mathbb{F}[V_i]$  for all  $i = 1, \dots, p-1$  we have  $\deg(m_1) > (p-1)^2$ , say. We use induction on  $\mu(m) := \max_{j=1}^n \deg(m_{1,j})$

If  $\mu(m) \geq p$  then let  $j$  be an index such that  $\deg(m_{1,j})$  is maximal and let  $x_1, \dots, x_p$  denote the variables in the coordinate ring  $\mathbb{F}[V_{1,j}]$ . For  $w := x_1 \cdots x_p$  there is a monomial  $v$  such that  $m - wv \in \mathbb{F}[W]_+^G \mathbb{F}[W]_+$  by Lemma 10. But  $wv \in \mathbb{F}[W]_+^G \mathbb{F}[W]_+$ , as  $w$  is invariant both under  $a$  and  $b$ , so we are done.

If  $\mu(m) < p$  then there is an index  $k \neq j$  such that  $\deg(m_{1,k}) > 1$ . Let  $y_1, \dots, y_p$  be the variables in the coordinate ring  $\mathbb{F}[V_{1,k}]$ . For  $w := x_1^{\mu(m)} y_1$  we have again by Lemma 10 a monomial  $v$  such that  $m - wv \in \mathbb{F}[W]_+^G \mathbb{F}[W]_+$ . For the monomial  $\tilde{w} = x_1^{\mu(m)+1}$  we have  $\tilde{w}v \in \mathbb{F}[W]_+^G \mathbb{F}[W]_+$  by the induction hypothesis. Now consider the polarisation operator  $\Delta_{k,j} := \sum_{i=1}^p y_i \partial_{x_i}$ . From the Leibniz rule it is obvious that  $\Delta_{k,j}$  takes  $\mathbb{F}[W]_+^G \mathbb{F}[W]_+$  into itself. As a result  $wv = (\mu(m) + 1)^{-1} \Delta_{k,j}(\tilde{w}v) \in \mathbb{F}[W]_+^G \mathbb{F}[W]_+$  where we have used our assumption on the characteristic of the base field  $\mathbb{F}$ .  $\square$

**Theorem 12.** *For any prime  $p \geq 5$  and base field  $\mathbb{F}$  of characteristic 0 or greater than  $p$  we have  $\beta(H_p) < p^2$ .*

*Proof.* The invariant ring  $\mathbb{F}[W]^{H_p}$  is spanned by its elements of the form  $\tau(m)$  where  $m$  is an  $A$ -invariant monomial and  $\tau : \mathbb{F}[W]^A \rightarrow \mathbb{F}[W]^{H_p}$  is the map given by the formula  $\tau(m) = \sum_{g \in H_p/A} m^g$  (see e.g. [13, Chapter 2.2]). By comparing Proposition 11 and Proposition 8 we see that any monomial  $m \in \mathbb{F}[W]^A$  with  $\deg(m) \geq p^2$  belongs to the ideal  $\mathbb{F}[W]_+^G \mathbb{F}[W]_+$ . As  $\tau$  is an  $\mathbb{F}[W]^{H_p}$ -module homomorphism we conclude that  $\tau(m) \in (\mathbb{F}[W]_+^{H_p})^2$ .  $\square$

## 4 The case $p=3$

**Proposition 13.** *Consider  $V = V_\omega$  for a primitive third root of unity  $\omega \in \mathbb{C}$  as given by (7). Then  $\beta(H_3, V) \geq 9$ .*

*Proof.* Let  $\mathbb{C}[V] = \mathbb{C}[x, y, z]$  with the variables chosen according to our conventions.  $\mathbb{C}[V]^{H_3}$  is spanned by the elements  $\tau(m) = \frac{1}{3}(m + m^b + m^{b^2})$  where  $m$  is an  $A$ -invariant monomial. An easy argument shows that  $xyz, x^3, y^3, z^3$  are the only irreducible  $A$ -invariant monomials. Set  $R = \mathbb{C}[xyz, \tau(x^3), \tau(x^3y^3)]$ . All  $A$ -invariant monomials of degree at most 8 have degree 3 or 6 and by enumerating them we see that  $\mathbb{C}[V]_d^{H_3} = R_d$  for all  $d \leq 8$ . So if we assume that  $\beta(H_3, V) \leq 8$  then we have  $\mathbb{C}[V]^{H_3} = R$ . Observe however that all the generators of  $R$  are symmetric polynomials, hence  $R \subset \mathbb{C}[V]^{S_3}$ . On the other hand  $\tau(x^6y^3) \in \mathbb{C}[V]^{H_3}$  is not a symmetric polynomial, whence necessarily  $\tau(x^6y^3) \notin R$ . This is a contradiction which proves that  $\beta(H_3, V) \geq 9$ .  $\square$

We will prove now some analogues of Proposition 8, Lemma 9, Lemma 10 and Proposition 11 which hold for the case  $p = 3$  with slight modifications:

**Proposition 14.** *If  $\text{char}(\mathbb{F}) \neq 3$  then  $\beta(H_3) \leq 9$ .*

*Proof.* Suppose for a contradiction that there is a monomial  $m \in \mathbb{F}[W]^A$  with  $\deg(m) \geq 10$  such that  $m \notin \mathbb{F}[W]_+^G \mathbb{F}[W]_+$ . Let  $S = \Phi_c(m)$ , identify  $\langle c \rangle$  with  $\mathbb{Z}/3\mathbb{Z}$  and let  $d_i = v_i(S)$  for  $i = 0, 1, 2$ . Assume by symmetry that  $d_1 \geq d_2$ .

**A.** *We must have  $h(S) \geq 5$ .*

$S$  is a zero-sum sequence over  $\mathbb{Z}/3\mathbb{Z}$  and this is only possible if  $d_1 - d_2 \equiv 0 \pmod{3}$ . So let  $d_1 - d_2 = 3k$  for some integer  $k \geq 0$ . Denoting by  $\ell(S)$  the maximum number of non-empty zero-sum sequences into which  $S$  can be factored we have  $\ell(S) = d_0 + d_2 + k \leq 5$  as otherwise by Lemma 3 we get  $m \in (\mathbb{F}[W]_+^c)^6 \subset \mathbb{F}[W]_+^G \mathbb{F}[W]_+$ , since  $D(C_3^2) = 5$  by (2). In particular  $d_0 \leq 5$ . On the other hand  $|S| = d_0 + d_1 + d_2 \geq 10$ . Subtracting from this inequality the previous one yields  $d_1 - k \geq 5$ , whence  $h(S) = d_1 \geq 5$ .

**B.** For any  $w \mid m_1$  with  $\deg(w) \leq 2$  there is a factorisation  $m = u_1 u_2 u_3$  with  $u_i \in \mathbb{F}[W]_+^A$  such that  $w \mid u_3$  and  $y \mid u_1 u_2$  for some variable  $y \mid m_1$ .

As  $\deg(m/w) \geq 8 = D_2(C_3^2)$  there is a factorisation  $m/w = u_1 u_2 t$  with  $u_1, u_2 \in \mathbb{F}[W]_+^A$ . Setting  $u_3 = tw$  enforces  $u_3 \in \mathbb{F}[W]_+^A$ . Here  $\deg(u_3) \leq D(A) = 5$  as otherwise  $u_3 \in (\mathbb{F}[W]_+^A)^2$  and  $m \in (\mathbb{F}[W]_+^A)^2 \subset \mathbb{F}[W]_+^G \mathbb{F}[W]_+$  by Lemma 3, a contradiction. Therefore we cannot have  $m_1 \mid u_3$  for then  $m_1 = u_3$  and  $\Phi_c(m_1) = (1^5)$  so that  $\Phi(u_3)$  is not a zero-sum sequence over  $A$ , a contradiction. So there is a variable  $y$  in  $\gcd(m_1, u_1 u_2)$  as claimed.

**C.** For any monomial  $w \in \mathbb{F}[V_1]$  with  $\deg(w) \leq p$  and  $\deg(w) \leq \deg(m_1)$  there is a monomial  $v \in \mathbb{F}[W]$  such that  $m - vw \in \mathbb{F}[W]_+^G \mathbb{F}[W]_+$ .

This follows from the proof of Lemma 10 using part **B** instead of Lemma 9 to produce the factorisation  $m = u_1 \cdots u_p$  needed in that argument.

**D.** Now we proceed by a case-by-case analysis as in [2, Section 2.4]:

1) If  $\deg(m_{1,i}) \geq 3$  for some  $1 \leq i \leq n$  then denoting by  $x_i, y_i, z_i$  the variables of  $\mathbb{F}[V_{1,i}]$  we can apply **C** with  $w := x_i y_i z_i \in \mathbb{F}[W]_+^G$  concluding that  $m \in \mathbb{F}[W]_+^G \mathbb{F}[W]_+$ , so that  $\tau(m) \in (\mathbb{F}[W]_+^{H_3})^2$  as before.

2) Otherwise if  $\deg(m_{1,i}) = 2$  for some  $i$  then still there is a  $j \neq i$  such that  $\deg(m_{1,j}) \geq 1$ . Then after an application of **C** we may assume that  $m$  is divisible by  $u := x_i^2 x_j$ . But  $m = \frac{1}{3} \Delta_{j,i}(m')$  for the monomial  $m' := m x_i / x_j$  which falls under case 1) so we are done again.

3) Finally, if  $\deg(m_{1,1}) = \dots = \deg(m_{1,n}) = 1$  then after an application of **C** we may assume that  $x_1 y_2 z_3 \mid m$ . Now consider the relation:

$$\Delta_{2,1}(x_1 y_1 z_3) + \Delta_{3,2}(x_1 y_2 z_2) + \Delta_{1,3}(x_3 y_2 z_3) = 3x_1 y_2 z_3 + \tau(x_3 y_2 z_1) \quad (13)$$

After multiplying (13) with  $m' = m / x_1 y_2 z_3$  we get on the left hand side  $\Delta_{2,1}(m y_1 / y_2) + \Delta_{3,2}(m z_2 / z_3) + \Delta_{1,3}(m x_3 / x_1) \in \mathbb{F}[W]_+^G \mathbb{F}[W]_+$  as all the three monomials occurring here fall under case 2). This completes our proof.  $\square$

Now comparing Proposition 13 and 14 immediately gives:

**Corollary 15.** If  $\text{char}(\mathbb{F}) \neq 3$  then  $\beta(H_3) = 9$ .

**Remark 16.** It would be interesting to know if Theorem 12 also extends to the whole non-modular case, i.e. for any field  $\mathbb{F}$  whose characteristic does not divide  $|G|$ , just as it is the case for  $p = 3$  by the above result.

## Acknowledgements

The author is grateful to Mátyás Domokos for many valuable comments on the manuscript of this paper. This work was partially supported by the National Research, Development and Innovation Office (NKFIH) grants PD113138, ERC HU 15 118286, K115799 and K119934.

## References

- [1] Y. Berkovich. *Groups of Prime Power Order*, volume I of *de Gruyter Expositions in Mathematics*. de Gruyter, Berlin, New York, 2008.
- [2] K. Csiszter, M. Domokos. *Groups with large Noether bound*, Ann. de l'Institut Fourier 64:(3) pp. 909-944. (2014)
- [3] K. Csiszter, M. Domokos. *The Noether number for the groups with a cyclic subgroup of index two*, Journal of Algebra 399: pp. 546-560. (2014)
- [4] K. Csiszter, M. Domokos. *On the generalised Davenport constant and the Noether number*, Central European Journal of Mathematics 11:(9) pp. 1605-1615. (2013)
- [5] K. Csiszter, M. Domokos, A. Geroldinger: *The interplay of Invariant Theory with Multiplicative Ideal Theory and with Arithmetic Combinatorics*, arXiv:1505.06059
- [6] H. Derksen, G. Kemper. *Computational Invariant Theory*, volume 130 of *Encyclopedia of Mathematical Sciences*. Springer-Verlag, 2002.
- [7] M. Domokos, P. Hegedűs. *Noether's bound for polynomial invariants of finite groups* Arch. Math. (Basel) 74 (2000), no. 3, pp. 161-167.
- [8] P. Fleischmann. *The Noether bound in invariant theory of finite groups*. Ad. Math., 156(1):23-32, 2000.
- [9] A. Geroldinger, F. Halter-Koch. *Non-unique factorizations. Algebraic, combinatorial and analytic theory*. Monographs and Textbooks in Pure and Applied Mathematics, Chapman & Hall/CRC, 2006.
- [10] F. Halter-Koch. *A generalization of Davenport's constant and its arithmetical applications*. Colloquium Mathematicum 63 (1992), 203-210.
- [11] P. Hegedűs, L. Pyber. *Upper bounds for the Noether number of a finite group* manuscript
- [12] F. Knop. *On Noether's and Weyl's bound in positive characteristic*. In H. E. A. E. Campbell and D. L. Wehlau, editors, *Invariant Theory in All Characteristics*, volume 35 of *CRM Proceedings and Lecture Notes*. Amer. Math. Soc., Providence, Rhode Island, 2004.

- [13] M. D. Neusel, L. Smith. *Invariant Theory of Finite Groups*. Mathematical Surveys and Monographs 94. Providence, R.I.: American Mathematical Society, 2002
- [14] E. Noether. *Der Endlichkeitssatz der Invarianten endlicher Gruppen*. Math. Ann., 77:89-92, 1916
- [15] J. E. Olson. *A combinatorial problem on finite Abelian groups. I*. J. Number Theory 1 (1969), 8–10.
- [16] J. E. Olson. *A combinatorial problem on finite Abelian groups. II*. J. Number Theory 1 (1969), 195–199.
- [17] B. J. Schmid. *Finite groups and invariant theory*. In Malliavin M. P., editor, *Topics in invariant theory*, number 1478 in Lecture notes in mathematics, pages 35–66. Springer, 1989-90.
- [18] J. P. Serre. *Representations linéaires des groupes finis*. Hermann, Paris, 1998.
- [19] M. Sezer. *Sharpening the generalized Noether bound in the invariant theory of finite groups*. J. Algebra 254 (2002), no. 2, 252263.